

# 基于双混沌置乱和扩频调制的彩色图像盲水印算法

胡裕峰 朱善安

(浙江大学 电气工程学院, 浙江 杭州 310027)

**摘要** 提出了一种新的适应彩色图像的盲水印算法, 先对宿主图像的绿色分量以  $8 \times 8$  像素分块进行离散余弦变换(DCT)变换, 用 logistic 映射生成两个混沌序列, 然后用混沌序列置乱加密二值水印图像, 并用两个互不相关的伪随机序列扩频调制水印, 最后将调制好的水印嵌入到 DCT 变换域的中频子带系数上, 进行分块 DCT 反变换得到水印化图像。提取水印时, 通过比较两个伪随机序列和水印化图像的相关性大小来提取水印, 不需要原始图像的参与, 为盲提取水印算法。实验结果证明本文算法能有效地抵抗 JPEG 压缩、加噪、剪切等常见攻击, 绿色分量嵌入水印比红色和蓝色分量嵌入水印能更好地抵抗 JPEG 压缩的攻击。

**关键词** 信息光学; 数字水印; 双混沌置乱; 扩频调制; 绿色分量; 盲水印

**中图分类号** TP390.7 **文献标识码** A **doi**: 10.3788/AOS20082809.1691

## Color Image Blind Watermark Algorithm Based on Double Chaotic Scrambling and Spread Spectrum Modulation

Hu Yufeng Zhu Shan'an

(College of Electrical Engineering, Zhejiang University, Hangzhou, Zhejiang 310027, China)

**Abstract** A new blind watermark algorithm for color image was proposed. First, the green component of the original image was blocked by size  $8 \times 8$  pixels and transformed with discrete cosine transformation (DCT). Second, two chaotic sequences were generated by logistic mapping, and the binary watermark image was scrambled by the chaotic sequences and spread spectrum modulated by two uncorrelated random sequences. Third, the modulated watermark was embedded in mid-frequency region coefficients of DCT domain. At last, the watermarked image was obtained by inverse discrete cosine transform. The watermark was extracted by comparing the correlation between two random sequences with watermarked image, the process did not need the original image, namely a blind watermark algorithm. Experimental results demonstrated that this method is invisible and robust against some usual attacks such as JPEG compression, cropping, adding noise, and embedding watermark in green component is more robust against lossy compression than embedding watermark in red or blue component.

**Key words** information optics; digital watermarking; double chaotic scrambling; spread spectrum modulation; green component; blind watermark

## 1 引 言

数字水印技术(Digital watermarking)<sup>[1~4]</sup>是近十年来多媒体内容保护领域的研究热点之一, 它将不可察觉的信号嵌入到多媒体内容中, 使其在发布传播后, 能从中提取出这些信息用于版权保护。目前, 彩色图像是当前图片内容传播的主流, 如何在彩色图像中合适地嵌入水印值得深入研究。Kutter

M 等<sup>[5]</sup>根据人眼对蓝色分量变换不敏感的特性, 提出了一种在彩色图像空间域蓝色分量嵌入水印的方案。但是彩色图像所占空间大, 传播时一般都经 JPEG 压缩处理, 经压缩后红、蓝色分量损失的能量大, 在这两个颜色分量嵌入水印, 水印信息相对损失也较大, 不易提取, 而绿色分量损失的能量相对较小, 因此将水印嵌入到绿色分量是一种较好的选择。

收稿日期: 2007-12-19; 收到修改稿日期: 2008-04-28

作者简介: 胡裕峰(1982-), 男, 博士研究生, 主要从事图象处理、数字水印技术和多媒体内容保护等方面的研究。

E-mail: huyufeng0726@163.com

导师简介: 朱善安(1952-), 男, 教授, 博士生导师, 主要从事预测自适应控制理论与工业应用、图像处理及模式识别和网络实验室等方面的研究。E-mail: zsa@zju.edu.cn (通信联系人)

目前的水印嵌入技术主要分为空域和变换域水印技术两类。空域嵌入水印,水印信息容量大,计算复杂度低,但稳健性差。变换域水印算法稳健性强,是研究的主流,它主要包括 DFT 变换、离散余弦变换(DCT)变换、离散小波变换(DWT)变换等方法。变换域图像的能量主要集中在低频部分, DCT 变换后的图像能明确地分为低(FL)、中(FM)、高(FH)三种频带区域<sup>[6]</sup>。低频区域是影响图像视觉效果的最重要区域,人眼对这部分的变化最敏感;高频区域是人眼最不敏感区域,将水印信息嵌入到此区域能达到很好的视觉透明效果,但是此区域正是压缩时量化步长最大的区域,各种常见的图像操作如有损压缩等对其损失很大,水印信息很容易丢失。综合比较,在中频区域嵌入水印能避免图像的严重失真和增强抗有损压缩的能力,是比较好的选择。

本文提出了一种新的水印算法:二值水印图像经双混沌序列置乱加密后,经两个互不相关的伪随机序列扩频调制嵌入到宿主图像绿色分量的 DCT 变换域的中频子带系数上。

## 2 选择绿色分量

RGB 彩色图像 JPEG 压缩时需经过颜色转换、DCT 变换、量化、编码、颜色转换五步。JPEG 只支持 YUV 颜色模式的数据结构,而不支持 RGB 图像数据结构,RGB 彩色图像进行压缩之前,按(1)式将图像从 RGB 模型转换到 YUV 模型<sup>[7]</sup>:

$$\begin{cases} Y = 0.299R + 0.587G + 0.114B, \\ U = -0.169R - 0.3313G + 0.5B, \\ V = 0.5R - 0.4187G - 0.0813B, \end{cases} \quad (1)$$

其中,  $Y$  表示亮度,  $U$  和  $V$  表示颜色。

转换完成之后还需要进行数据采样,然后再量化。一般采用的采样比例是 2:1:1 或 4:2:2。由(1)式可见,占采样比例大的最重要的亮度部分绿色分量明显高于红色和蓝色分量,因此 JPEG 压缩时,绿色分量信息保存最多,所以选择在绿色分量嵌入水印信息,稳健性更强。进一步分析,还可直接在 YUV 模型中嵌入水印,但为了避免模型空间转换时小数取整误差,本文直接选择绿色分量嵌入。

## 3 水印图像的双混沌置乱和扩频调制

目前常用的水印图像置乱方法包括基于 Magic 变换、Arnold 变换的置乱等<sup>[8,9]</sup>,它们都能实现对图像的加密,但它们的密钥空间较小,而且置乱矩阵是

有周期的,经过置乱后的图像,再继续多次变换后会恢复成原图像。这样在加密算法公开时,攻击者易破解恢复水印图像,安全性能不高。本文利用混沌序列对初值的敏感性高,安全性强,密钥空间大,而且是非周期的特性,产生两个混沌序列分别置乱水印图像的行和列,加密图像。

### 3.1 混沌序列的生成

一种简单且广泛应用的混沌序列可由 Logistic 映射<sup>[10]</sup>来生成

$$s_{i+1} = \mu s_i (1 - s_i), \quad i = 0, 1, 2, \dots \quad (2)$$

其中  $\mu$  为分支参量,取值范围为  $[0, 4]$ , 初始值选为  $0 < s_0 < 1$ , 得到的序列为单极性的,且  $0 < s_i < 1$ 。研究表明,  $3.5699456 \dots < \mu \leq 4$  时, Logistic 映射工作于混沌态,它产生的序列非周期、非收敛、对初始值十分敏感,本文选择  $\mu = 4$ 。

### 3.2 水印图像的双混沌序列置乱

对一  $64 \text{ pixel} \times 64 \text{ pixel}$  的二值水印图像,可用矩阵表示为  $\{S(m, n)\}$ , ( $m = 0, 1, \dots, 64, n = 0, 1, \dots, 64$ ), 先置乱图像的行,算法如下:

1) 任意给定一有效位为 14 位的初始值  $x_0$  ( $0 < x_0 < 1$ ), 利用 Logistic 映射经过  $L$  ( $1000 \leq L$ ) 步迭代去除混沌暂态得到新的初始值  $x_0$ , 初始化数组  $P_i$ , ( $i = 1, 2, 3, \dots, 64$ ) 的值均为 0, 下标  $i = 1$ 。

2) 对  $x_0$  进行以下运算:

$$\alpha = E[\text{mod}(x_0 \times 10^{14}, 64) + 1], \quad (3)$$

其中  $\text{mod}$  为求余运算,  $E[\cdot]$  表示向下取整, 得到的  $\alpha \in [1, 64]$ , 且为整数, 令  $p_1 = \alpha, i = i + 1$ 。

3) 将  $x_0$  代入(2)式得到新的  $x_0$ , 代入(3)式得到新的  $\alpha$ , 如果  $\alpha \notin P_i$ , ( $i = 1, 2, 3, \dots, 64$ ), 则令  $p_i = \alpha, i = i + 1$ 。

4) 直到下标  $i = 65$ , 迭代停止, 否则转步骤 3)。

通过上述迭代的算法填充数组  $P$ , 该数组中的值两两不相同, 且为属于  $[1, 64]$  的整数, 因此可以利用此数组来置乱水印图像矩阵的行。置换规则如下:

$$F(m, :) = S(i, :), \quad m = P[i] \quad (4)$$

即将水印图像矩阵的第  $i$  行置换为  $F$  的第  $m$  行,  $F(m, :)$  为行置乱后的水印图像矩阵。

在行置乱的基础上, 对矩阵  $F$ , 用另一初始值  $y_0$  重复上述行置乱的步骤进行列置乱得到双混沌序列置乱后的水印图像矩阵  $W$ , 任意给定的初始值  $x_0, y_0$  作为水印置乱的密钥, 在水印提取的时候要用到。

### 3.3 水印的扩频调制

对置乱后的水印图像矩阵  $W$  进行从左到右、从上至下逐行扫描, 生成一维序列  $W' \in \{0, 1\}, i = 1,$

2, 3, \dots, 64 \times 64。由图 1 得到图像 8 pixel \times 8 pixel 块 DCT 变换后中频区域有 22 个像素, 先按照以下规则生成两个伪随机序列  $R_0$  和  $R_1$ 。

$$\begin{cases} R_0 = \{r_{0k} \mid r_{0k} \in \{-1, 0, 1\}, \\ \quad k = 1, 2, 3, \dots, 22\} \\ R_1 = \{r_{1k} \mid r_{1k} \in \{-1, 0, 1\}, \\ \quad k = 1, 2, 3, \dots, 22\} \end{cases} \quad (5)$$

$$\frac{1}{22} \sum_{k=1}^{22} r_{0k} = 0, \quad \frac{1}{22} \sum_{k=1}^{22} r_{1k} = 0, \quad \sum_{k=1}^{22} r_{0k} \times r_{1k} = 0$$

即  $R_0$  和  $R_1$  是均值为零、互不相关的伪随机序列。

$W'$  的每一位用两个伪随机序列进行扩频调制, 其中“0”以  $R_0$  表示, “1”以  $R_1$  表示, 并将每一位如图 1 所示扩充为  $8 \times 8$  的矩阵  $W'_j(u, v)$ , 其中 FL 和 FH 区域元素都填为 0, 伪随机序列  $R_0$  或  $R_1$  的元素按照从左至右、从上至下的顺序依次填入 FM 区域。

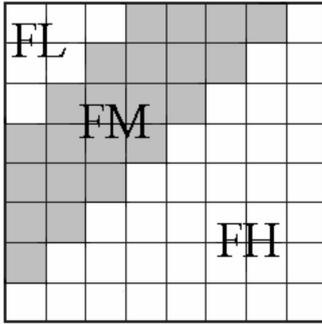


图 1 DCT 变换后频带区域

Fig. 1 Frequency region of DCT

## 4 水印的嵌入和提取

### 4.1 水印的嵌入

水印嵌入的步骤:

- 1) 提取原始 RGB 图像的绿色分量  $G$ 。
- 2) 对绿色分量按照  $8 \text{ pixel} \times 8 \text{ pixel}$  分块, 分别进行 DCT 变换得到  $B_j(u, v)$ , 下标  $j$  表示第几块。
- 3) 按(6)式加性嵌入水印,

$$B_{w_j}(u, v) = \begin{cases} B_j(u, v) + K \times W'_j(u, v), & u, v \in \text{FM} \\ B_j(u, v), & u, v \notin \text{FM} \end{cases} \quad (6)$$

式中  $K$  为嵌入强度。

4) 对  $B_{w_j}(u, v)$  进行 IDCT 变换得到水印化图像的绿色分量, 和原图像的红、蓝分量合成水印化 RGB 图像。

### 4.2 水印的无源提取

提取水印时不需要原始图像的参与, 根据相关

值大小关系来重构水印。水印提取的步骤:

- 1) 提取水印化 RGB 图像的绿色分量  $G'$ 。
- 2) 对绿色分量按照  $8 \text{ pixel} \times 8 \text{ pixel}$  分块, 分别进行 DCT 变换得到  $B'_{w_j}(u, v)$ , 取各块的中频区域系数  $B'_j(u, v)$ , ( $u, v \in \text{FM}$ ), 按从左至右、从上至下的顺序重排列每个中频系数为一维序列  $B'_j(m)$ , ( $m = 1, 2, 3, \dots, 22$ ), 上面提到的下标  $j$  表示第几块。
- 3) 分别计算中频系数一维序列和伪随机序列  $R_0$  和  $R_1$  的相关值, 按(7)式来确定提取水印的位值:

$$W_j = \begin{cases} 0, & \text{Corr2}(R_0, B'_j) > \text{Corr2}(R_1, B'_j) \\ 1, & \text{Corr2}(R_0, B'_j) \leq \text{Corr2}(R_1, B'_j) \end{cases} \quad (7)$$

其中  $\text{Corr2}$  表示计算两者的相关值。

4) 将  $W_j$  重新排列成原二维水印图像大小, 并利用密钥  $x_0, y_0$  反置乱变换即得到提取的水印图像。

5) 水印提取出来后, 可通过主观视觉判断水印是否相同, 也可以比较提取的水印和原始水印的相似度, 定义相似度  $H = X/Y$ , 其中  $X$  表示两者元素相同个数,  $Y$  表示元素总数;

6) 给定一个阈值  $T$ , 如果  $H > T$ , 则认为待检测图像中含有原始水印, 否则水印不存在。

## 5 实验结果和分析

取大小为  $64 \text{ pixel} \times 64 \text{ pixel}$  的二值图像图 2(a) 作为原始水印图像。图 2(b) 为原始水印图像经过双混沌序列置乱得到的图像, 其中行置乱混沌初始值  $x_0$  为 0.2973512314155, 列置乱混沌初始值  $y_0$  为 0.6973512314155, 初始迭代的步数  $L = 1000$ 。图 2(c) 为用非正确密钥  $x_0 = 0.2973512314156$ ,  $y_0 = 0.6973512314156$  恢复置乱图像的效果。图 2(d) 为使用正确密钥恢复的图像。可以看出, 即使密钥有微小的差异也不能恢复原图像, 水印攻击者不知道密钥无法恢复水印图像。

本文中对置乱后的水印图像 2(b) 进行扩频调制的两个伪随机序列的取值分别为:

$$R_0 = [-1, 0, 1, -1, 0, 1, 0, 1, 0, 1, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1], R_1 = [0, -1, 1, -1, -1, -1, 0, 0, 1, -1, 0, 0, -1, 1, 0, 0, 1, 0, 1, 0, 1, 0]$$

图 3(a) 是大小为  $515 \text{ pixel} \times 512 \text{ pixel}$  的 256 级 RGB 彩色图像 Lena, 提取其绿色分量, 将绿色分成  $8 \text{ pixel} \times 8 \text{ pixel}$  大小的子块, 分块进行 DCT 变换, 在中频区域嵌入经置乱和扩频调制的水印图像, 然后 IDCT 变换得到水印化图像图 3(b), 图 3(c) 为

两者图像差扩大 20 倍的效果,可以看出水印能量平均分布在水印化图像各块区域。水印嵌入强度  $K=16$  (PSNR 为峰值信噪比<sup>[11]</sup>) 从图 3 可以看出,

人眼无法察觉原始图像和水印化图像的差别,证明本文算法能保证水印的透明性。

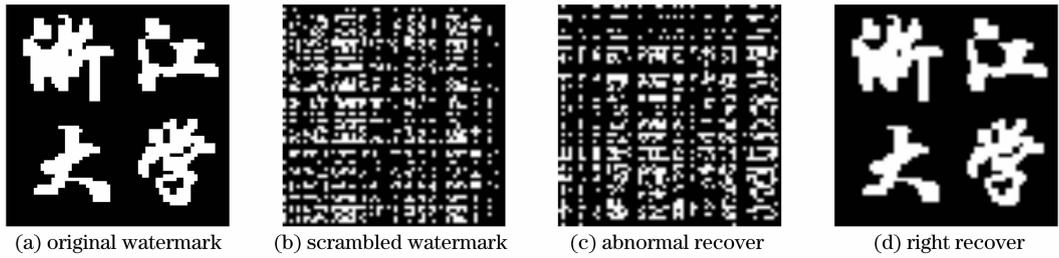


图 2 水印图像置乱及恢复实验。(a)原始水印,(b)置乱水印,(c)异常恢复,(d)正确恢复

Fig. 2 Scramble and recovery of watermark. (a) Original watermark, (b) scrambled watermark, (c) abnormal recovery, (d) right recovery



图 3 原始图像和水印化图像( $K=16$ ,  $PSNR=35.4$ )。(a)原始图像,(b)水印化图像,(c)差值图像

Fig. 3 Original image and watermarked image. (a) Original image, (b) watermarked image, (c) difference image

表 1 为从各种攻击提取出来的水印图像及它们与原始水印图像的相似度。可以看出,本文方法能有效抵抗 JPEG 压缩、加噪、剪切等常见攻击。当提取出来的水印相似度  $H$  等于 0.7905 时,人眼能够清晰地判断出提取的水印就是原始水印,证明采用

图像作为水印信息,在提取的时候更容易被人眼的自适应性来判断水印正确与否。剪切不同的区域,包括边缘、中央等,都能正确地提取出水印,这是因为采用混沌置乱把水印信息打散到图像的各个区域,剪切破坏的水印信息均匀分布在水印图像里面

表 1 各种攻击提取出来的水印图像及它们与原始水印图像的相似度

Table 1 Extracted watermarks from different attacked and H with original watermark

attack type	none	JPEG compression					
		Q=90	Q=80	Q=70	Q=60	Q=50	Q=40
$H$	0.9885	0.9761	0.9753	0.9666	0.9414	0.8853	0.7905
watermark							
attack type	Gaussian noise (0, 0.01)	Gaussian noise (0, 0.02)	salt noise (0.01)	salt noise (0.02)	crop edge	crop center	crop multi-region
$H$	0.9324	0.8779	0.9514	0.9087	0.9612	0.9592	0.9426
watermark							

而不是集中在一个区域。

表 2 给出了在宿主图像不同颜色分量嵌入同强度水印(K=16)抵抗 JPEG 有损压缩的性能实验数据。可以看出,不同的颜色分量嵌入水印,抵抗 JPEG 压缩攻击的性能差别很大。在同等强度水印、同等 JPEG 压缩因子,绿色分量嵌入提取的水印与原始水印的相似度最高,红色分量次之,蓝色分量最低。证明绿色分量抗 JPEG 压缩的稳健性最好,红色分量次之,蓝色分量很差。同时,也对不同颜色分量嵌入水印时进行加噪、剪切等攻击性试验,发现三个颜色分量对此类攻击的稳健性相差不大。主要是因为 JPEG 压缩时,对绿色分量影响最小,而对红、蓝色分量舍弃得较多,其它加噪、剪切等攻击的时候各个颜色分量受影响的程度相差不大。

表 2 不同颜色分量嵌入同强度水印(K=16)JPEG 压缩攻击提取的水印相似度比较

Table 2 Comparison of  $H$  in different color components under JPEG compression attack

JPEG compression attack	$H$		
	Red component	Green component	Blue component
Q=90	0.9331	0.9761	0.7915
Q=80	0.8933	0.9753	0.6782
Q=70	0.8179	0.9666	0.6157
Q=60	0.7253	0.9414	0.5737
Q=50	0.6599	0.8853	0.5532
Q=40	0.6035	0.7905	0.5186
Q=30	0.4514	0.6914	0.4251
Q=20	0.3533	0.5013	0.3124

图 4 为本文算法和文献[12]彩色水印算法在 JPEG 压缩攻击下提取水印相似度结果。可以看到,本文算法抗 JPEG 压缩能力明显高于文献[12],这是因为本文利用了绿色分量 JPEG 压缩时损失较少的特性。

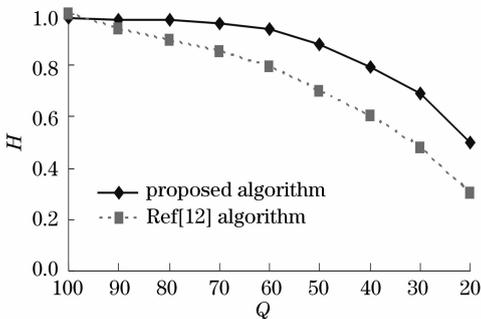


图 4 两种算法的抗 JPEG 压缩性能比较

Fig. 4 Comparison of two algorithms resisting JPEG compression

为了验证盲检测算法的可靠性,用随机序列发生器设计了 300 个不同的 64 pixel×64 pixel 的二值水印,并用本文水印替代第 200 个水印,分别嵌入到原始宿主图像,得到 300 个不同的水印化图像,然后分别对每个进行水印提取,计算提取出的水印与原始水印的相似度,如图 5 所示。可以看出只有水印化图像嵌入的是原始水印的时候,相似度才产生峰值,而其它随机水印相似度都在 0.5 附近很小地波动。

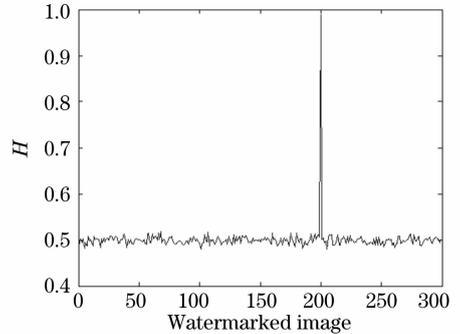


图 5 300 幅随机水印化图像检测出来的水印相似度  
Fig. 5 Similarity degree of watermark detected from stochastic 300 watermarked images

### 6 结 论

采用二值图像作为水印图像,通过双混沌序列置乱水印图像,将互不相关的两个伪随机序列扩频调制水印后,嵌入到彩色图像的绿色分量的中频系数中。实验结果表明,对加噪、剪切和 JPEG 压缩有很好的稳健性,在绿色分量嵌入水印抗 JPEG 有损压缩攻击的能力远远好于在红色分量和蓝色分量嵌入水印。提取水印的时候不需要原始图像的参与,为盲检测水印算法。由于采用双混沌序列置乱加密水印,攻击者在不知道密钥的情况下,不可能提取出水印,有很好的安全性,用伪随机序列扩频调制原水印增强了水印算法的稳健性。

### 参 考 文 献

- 1 I. J. Cox, M. L. Miller, J. A. Bloom. *Digital Watermarking* [M]. New York: Academic Press, 2002
- 2 Huang Qinglong, Liu Jianlan. Blind digital watermarking technique based on optical Fresnel diffraction[J]. *Acta Optica Sinica*, 2006, **26**(8): 1145~1149  
黄清龙, 刘建岚. 基于光学菲涅耳衍射的“盲数字水印”技术[J]. *光学学报*, 2006, **26**(8): 1145~1149
- 3 Yuchi Liang, Gu Jihua, Liu Wei *et al.*. An image digital watermark technique based on digital holography and discrete cosine transform[J]. *Acta Optica Sinica*, 2006, **26**(3): 355~361  
尉迟亮, 顾济华, 刘 薇 等. 基于数字全息及离散余弦变换的图

- 像数字水印技术[J]. 光学学报, 2006, **26**(3): 355~361
- 4 Peng Xiang, Bai Weidong, Tian Jindong. Digital watermarking with half-tone encoded computer generated hologram[J]. *Acta Optica Sinica*, 2007, **27**(6): 1011~1017  
彭 翔,白伟东,田劲东. 半色调编码计算全息图的数字水印方法[J]. 光学学报, 2007, **27**(6): 1011~1017
- 5 M. Kutter, F. Jordan, F. Bossen. Digital signature of colorimages using amplitude modulation[C]. *Proc. SPIE*, 1997, **3022**: 518~526
- 6 G. Langelaar, I. Setyawan, R. L. Lagendijk. Watermarking digital image and video data [J]. *IEEE Signal Processing Magazine*, 2000, **17**(9): 20~43
- 7 K. R. Castleman. *Digital Image Processing* [M]. New York: Prentice Hall, 1998
- 8 Ding Wei, Qi Dongxu. Digital image transformation and information hiding and disguising technology [J]. *Chin. J. Computers*, 1998, **21**(9): 838~843  
丁 玮,齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报, 1998, **21**(9): 838~843
- 9 Ding Wei, Yan Weiqi, Qi Dongxu. Digital image scrambling technology based on arnold transformation [ J ]. *J. Computer-Aided Design & Computer Graphics*, 2001, **13**(4): 338~341  
丁 玮,闫伟齐,齐东旭. 基于 Arnold 变换的数字图像置乱技术 [J]. 计算机辅助设计与图形学学, 2001, **13**(4): 338~341
- 10 Liu Ping, Yan Chuan, Huang Xiangao. Optimized method of generating the spread-spectrum sequences based on logistic-map [J]. *J. Communications*, 2007, **28**(2): 134~140  
柳 平,闫 川,黄显高. 改进的基于 Logistic 映射混沌扩频序列的产生方法[J]. 通信学报, 2007, **28**(2): 134~140
- 11 Stefan Katzenbeisser, Petitcolas Fabien, A. P. *Information Hiding Techniques for Steganography and Digital Watermarking* [M]. Northwood: Artec House, 1999. 97~119
- 12 Saraju P. Mohanty, Parthasarathy Guturu. A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion-extraction [ C ]. Proceedings of the Eighth IEEE International Symposium on Multimedia, San Diego, USA, 2006. 1145~1163